Cisco TrustSec How-To Guide: Guest Services

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

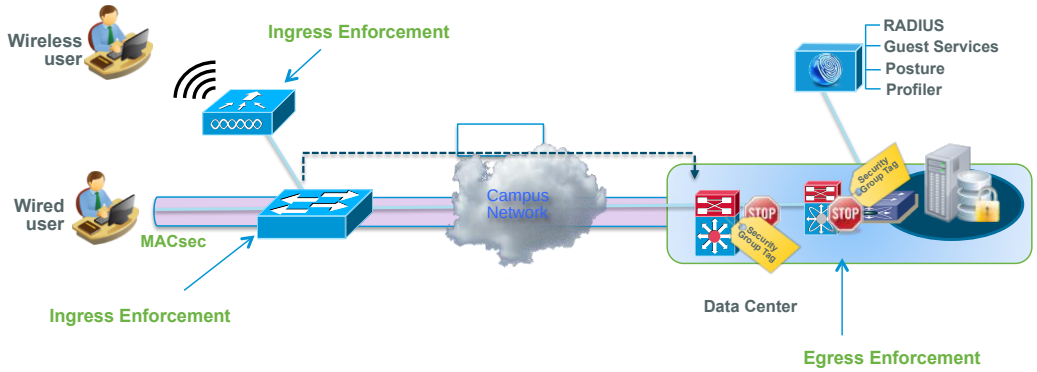
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

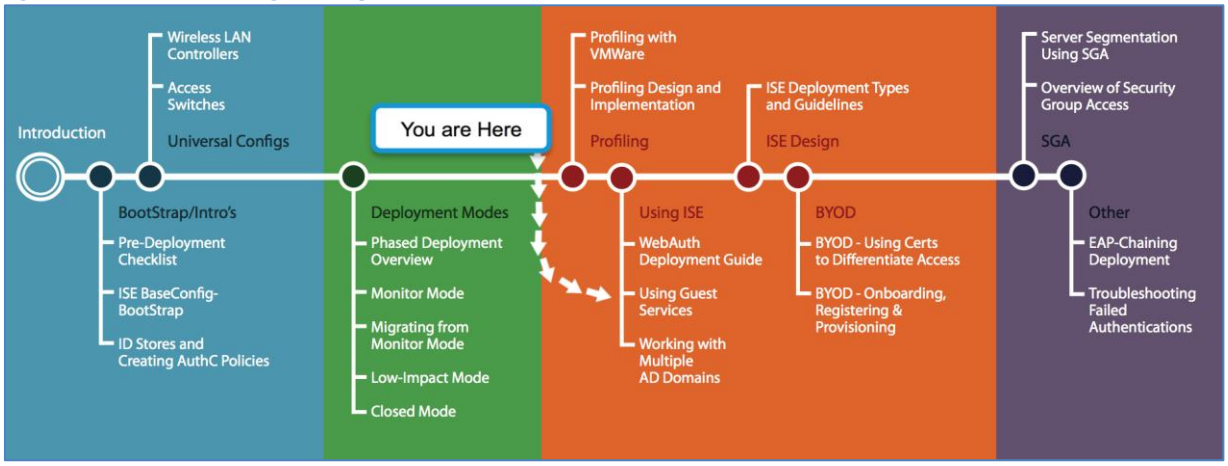


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "TrustSec "certified". The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Guest and Contractor Provisioning and Access

Overview

TrustSec helps organizations secure guest and contractor access to corporate networks, helping to ensure that guest and visitor traffic remains segregated from internal networks and assessing incoming computers for threats that may affect network availability and security. It also provides limited access for contractors to the internal network. Cisco® Identity Services Engine (ISE) offers centralized guest access management and enforcement for wired and wireless users, and can integrate easily with wireless solutions, third-party guest access portals, and billing providers.

Cisco ISE Guest Services allow guests, visitors, contractors, consultants, or customers to perform an HTTPS login to access a network, whether that network is a corporate intranet or the public Internet. The network is defined through a VLAN and/or a downloadable access control list (dACL) configuration in the network access device (NAD). Cisco ISE offers a simple client configurable Sponsor portal for creating and managing guest user accounts. ISE also supports default and customizable Guest Login portals to handle guest user login. Guest service provisions a guest account for the amount of time specified when the account is created.

Aside from the guest users, whom we define users as "users who simply need Internet-only access," we will also cover contractors, who need access to internal resources. The benefit of using the Cisco ISE to manage contractors is to provide management without having to provide main directory accounts such as Microsoft Active Directory (AD). Aside from the guest and contractor access, we will also define two different sponsor groups: one that can only create guest users, and the other that can create guest and contractor users.

In this How-To Guide, we will review the overall workflow for configuring ISE Guest Services, including sponsor setup, guest setup, contractor setup, and configuration of authorization policies for guest and contractor access.

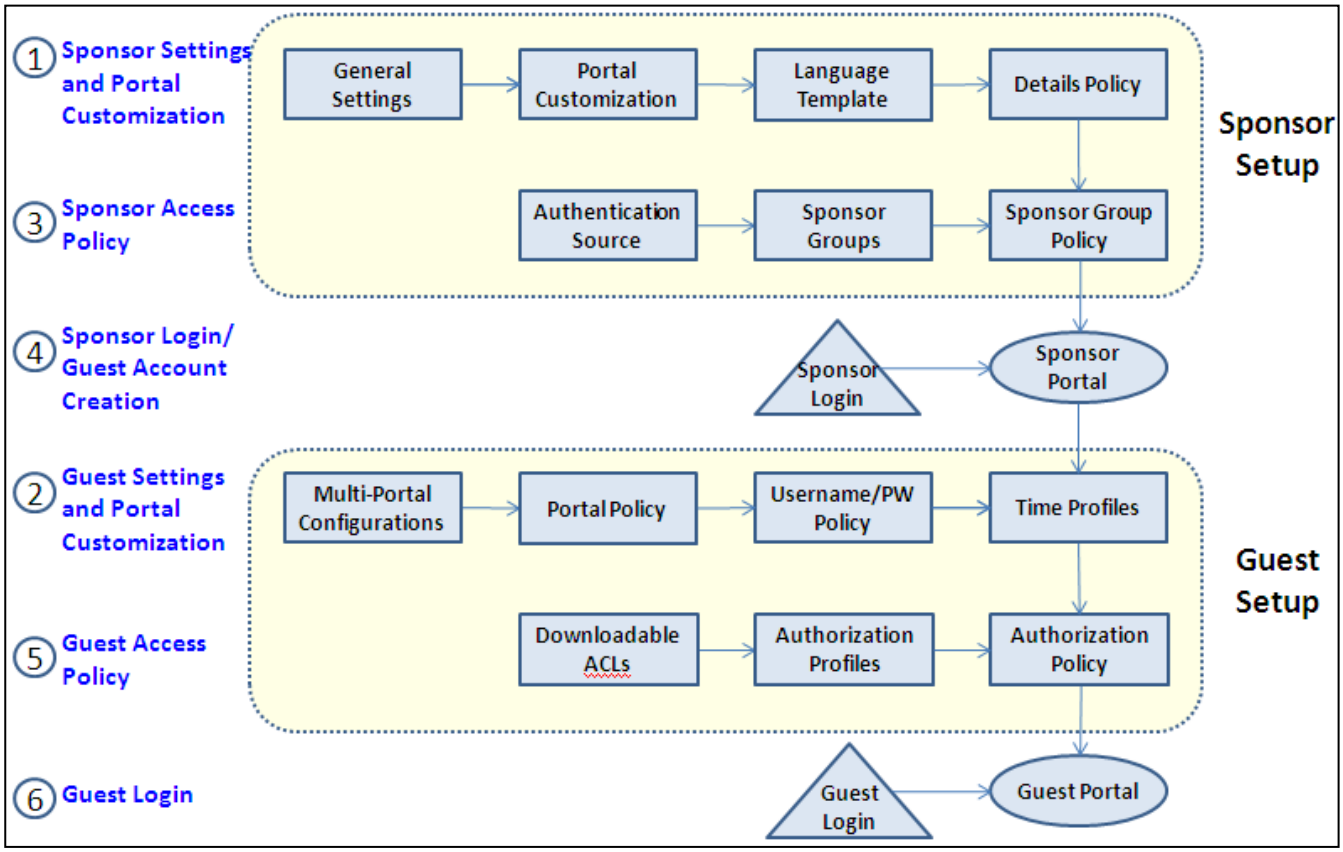
Using ISE Guest Services to Provision Multiple Roles

Cisco ISE Guest Services exposes two web portals, the Guest portal and Sponsor portal:

- Guest portal: Used for authenticating users via web browser, provides Acceptable Use Policy (AUP) [[ok?]] acknowledgment, changing of passwords, and self-registration
- Sponsor portal: Used for sponsors to create, update, and manage guest user accounts

Figure 3 shows the main steps in configuring guest services.

Figure 3 Guest Services Configuration Flow



Universal Guest Configuration: Sponsor User Configuration

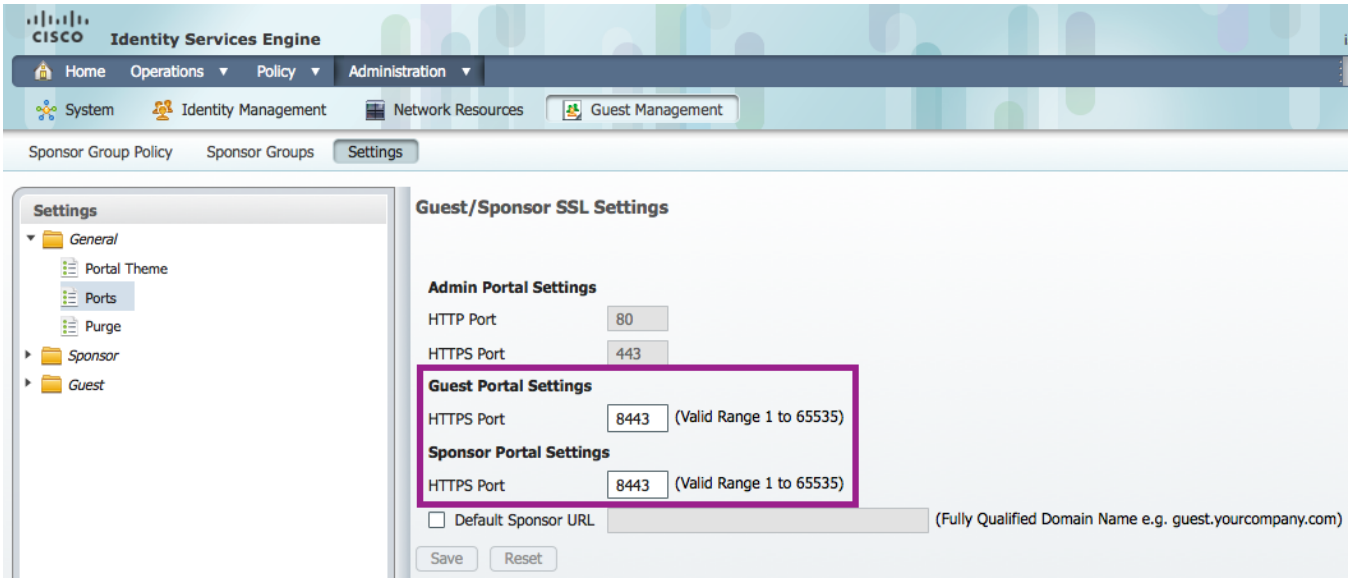
Procedure 1 Configure Sponsor System Settings

Step 1 Navigate to Administration → Guest Management → Settings → General → Ports.

Step 2 Verify the HTTPS ports used for portal access as required for the Guest and Sponsor portal.

Step 3 The default portal setting is 8443, as shown in Figure 4.

Figure 4 Guest and Sponsor HTTPS Port Settings

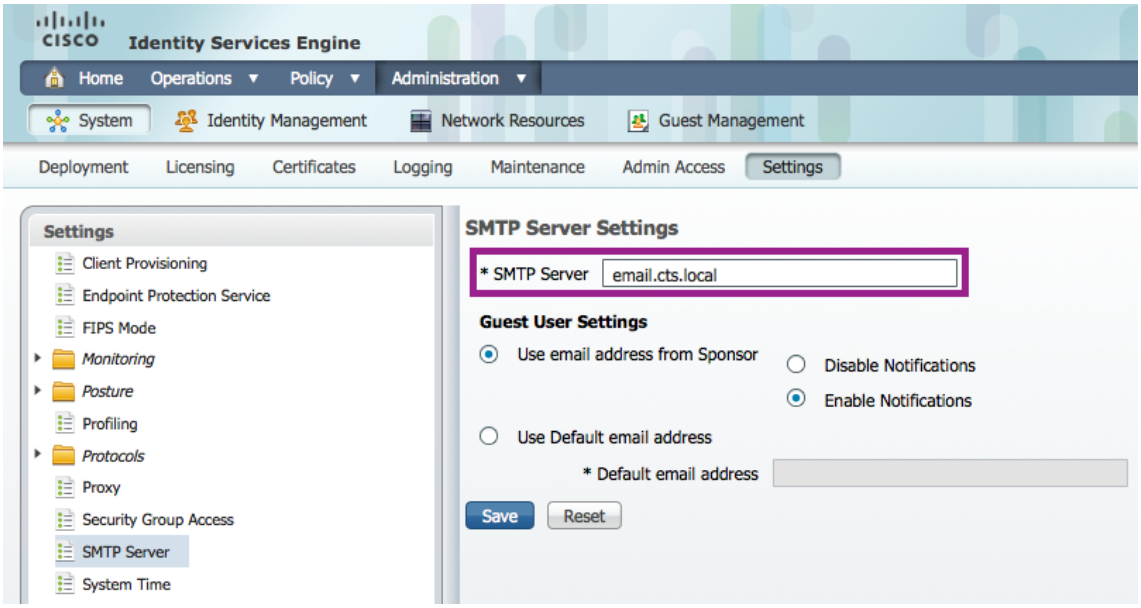


Step 4 (Optional) Click check box next to Default Sponsor URL and enter the common fully qualified domain name (FQDN) for Sponsor portal URL. This allows sponsors to reference Sponsor portal in a simple URL. Note that DNS must be configured to reference real node IP address for this common FQDN in order for this to work. In a distributed ISE deployment, it is recommended to use a load balancer for this web portal to provide redundancy.

Step 5 Navigate to Administration → System → Settings → SMTP Server.

Step 6 Enter your mail server and configure notification settings as required (Figure 5).

Figure 5 SMTP Server Settings



Procedure 2 Configure Guest Sponsor Groups

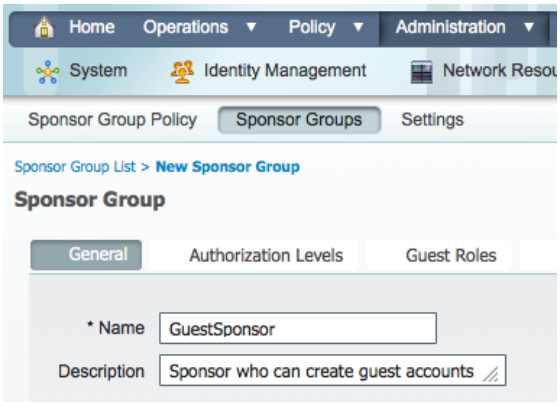
Step 1 The guest sponsor group contains the permissions and settings for the sponsor user.

Step 2 Navigate to Administration → Guest Management → Sponsor Groups.

Step 3 Click Add or Edit to create or edit a sponsor group.

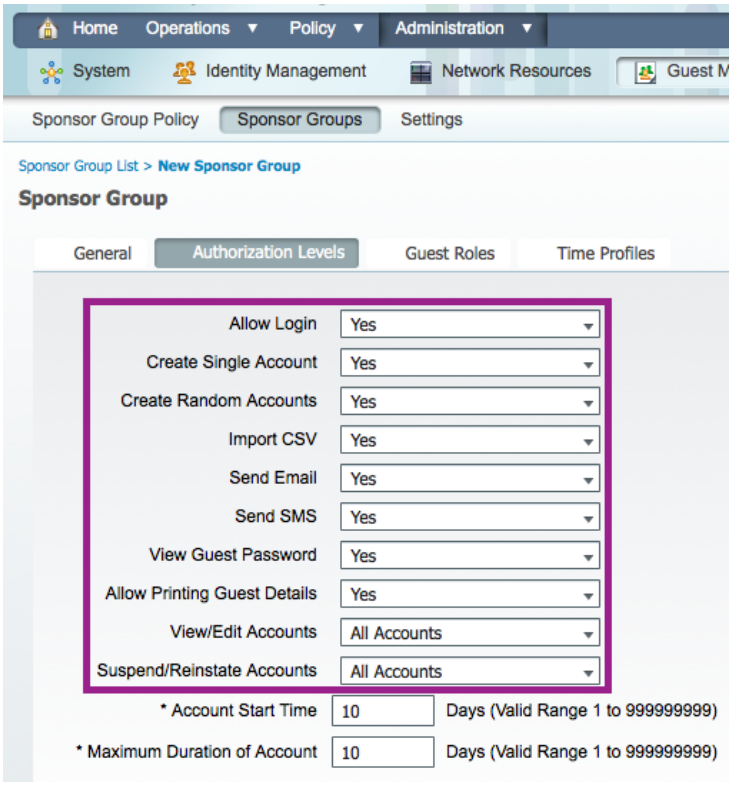
Step 4 Under the General tab, enter a name and description (Figure 6).

Figure 6 Creating the Sponsor Group for Guests



Step 5 Under the Authorization Levels tab, set permissions as necessary (Figure 7).

Figure 7 Setting Guest Sponsor Group Permissions



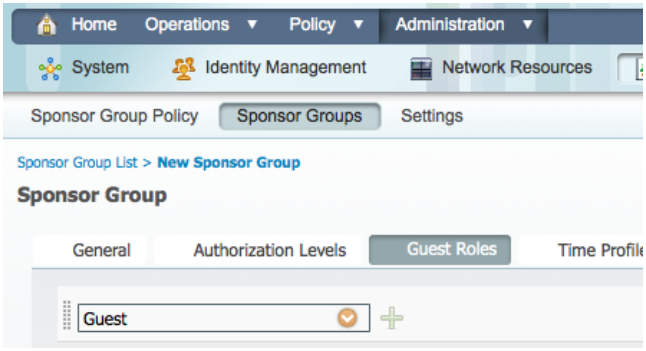
Step 6 Select the appropriate values for View/Edit Accounts, Suspend/Reinstate Accounts, Account Start Time, and Maximum Duration of Account settings.

Step 7 Example settings are shown in Figure 7 above.

Note: If the Maximum Duration of Account is less than the assigned Time Profile, the Maximum Duration of Account will be used instead of the Time Profile for guest account creation.

Step 8 From the Guest Roles tab, choose the guest roles that the sponsor group user is allowed to assign to the guest user (Figure 8).

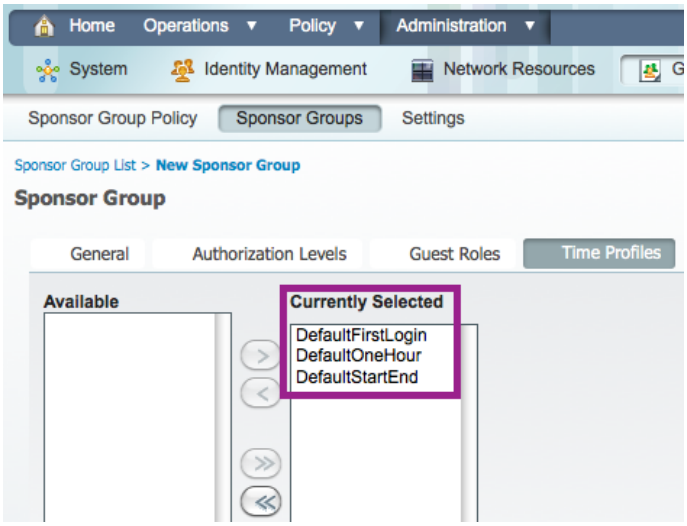
Figure 8 Setting Available Guest Roles for Guest Sponsor Group



Note: When guest users are created by a sponsor or through self-service, the guest account is not active until guest user logs in through Cisco ISE web portal. In ISE 1.1.1, there is a new default ID group for guests available named **ActivatedGuest.** The purpose of this group of guest accounts is to allow organizations to create guests that don't have to come to an ISE web portal before being able to pass authentication. This comes in handy if guest users are required to authenticate through a non ISE web portal such as Local Web Auth (LWA), 802.1X, and VPN.

Step 9 Under the Time Profiles tab, choose time profiles that the sponsor group user is able to assign to guest accounts (Figure 9).

Figure 9 Setting Available Time Profiles for Guest Sponsor Group



Step 10 Click Submit to save the configuration.

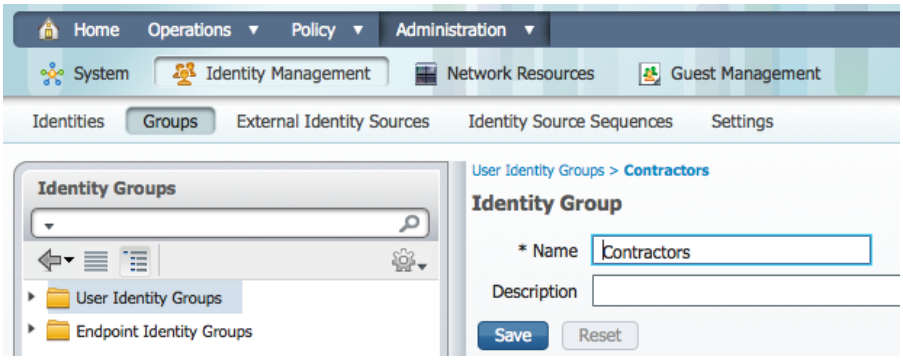
Procedure 3 Configure Identity Group for Contractors

Step 1 Create a separate user group for contractors.

Step 2 Navigate to Administration → Identity Management → Groups.

Step 3 Click Add to create a contractor group (Figure 10).

Figure 10 Creating a Contractor User Group



Step 4 Enter a name and description.

Step 5 Click Submit to save the configuration.

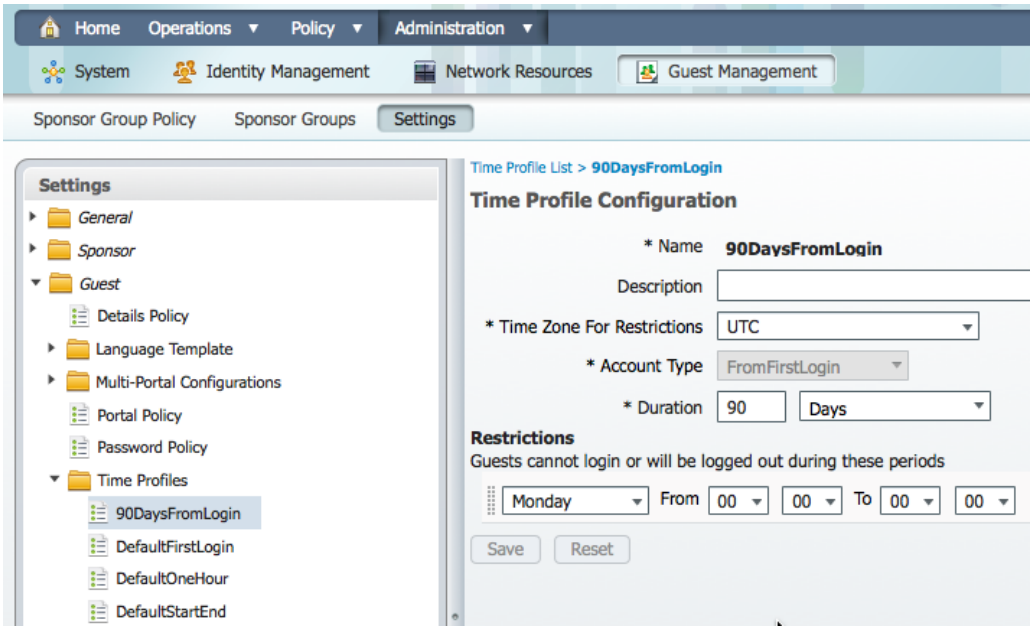
Procedure 4 Configure Time Profiles for Contractors

Step 1 Create a time profile that allows extended access for contractors.

Step 2 Navigate to Administration → Guest Management → Settings → Guest → Time Profiles.

Step 3 Click Add to create a time profile.

Figure 11 Configuring a Time Profile Configuration for Contractors



Step 4 Enter a Name, Description, and select Account Type and Duration.

Step 5 Click Submit to save the configuration.

Procedure 5 Configure Contractor Sponsor Groups

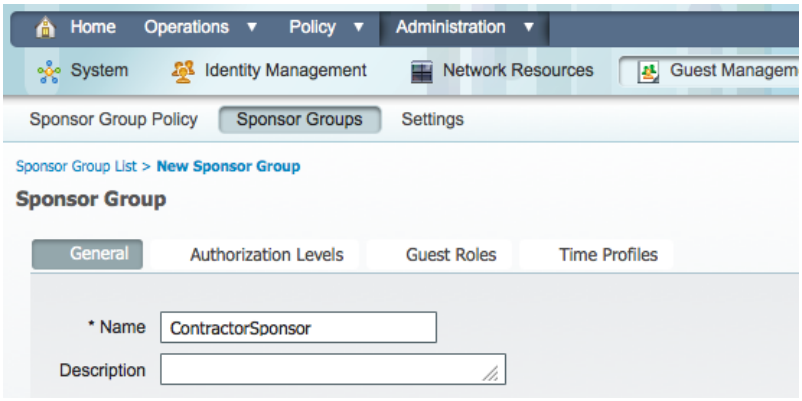
Step 1 The contractor sponsor group contains the permissions and settings for the sponsor user.

Step 2 Navigate to Administration → Guest Management → Sponsor Groups.

Step 3 Click Add to create a new sponsor group.

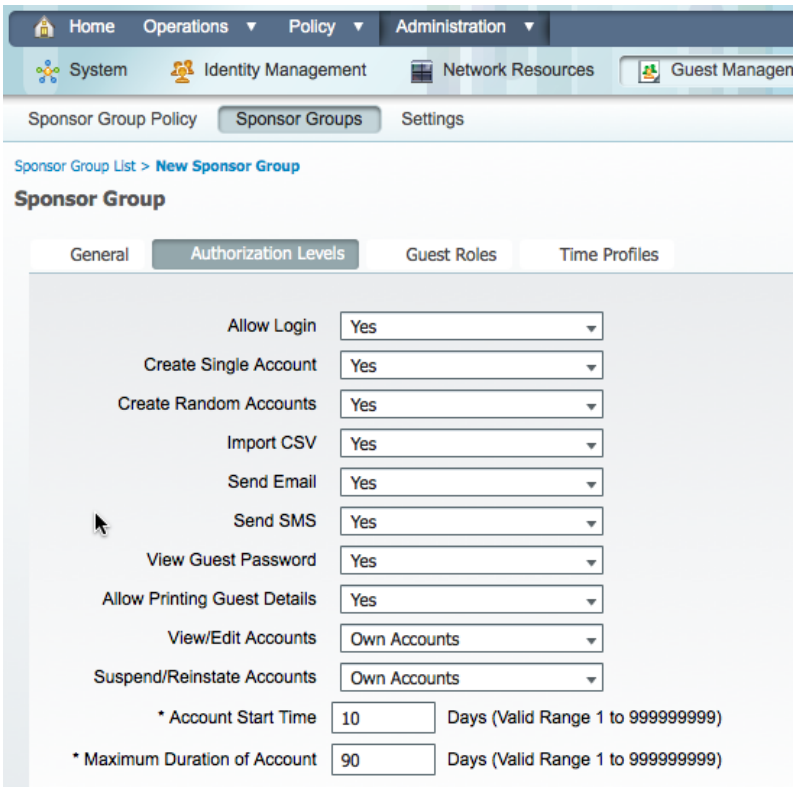
Step 4 Under the General tab, enter a name and description for the new group (Figure 12).

Figure 12 Creating a Contractor Sponsor Group



Step 5 Under the Authorization Levels tab, set permissions as necessary (Figure 13).

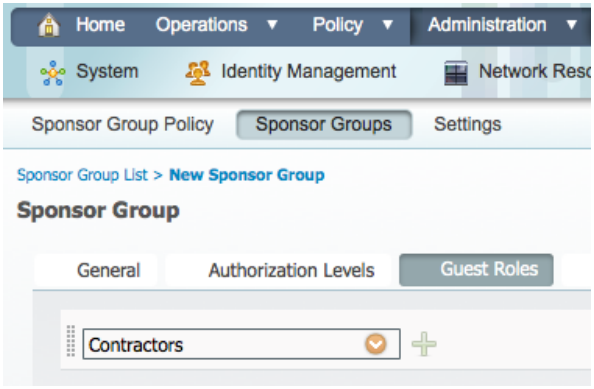
Figure 13 Setting Contractor Sponsor Group Permissions



Step 6 Select the appropriate values for View/Edit Accounts, Suspend/Reinstate Accounts, Account Start Time, and Maximum Duration of Account settings.

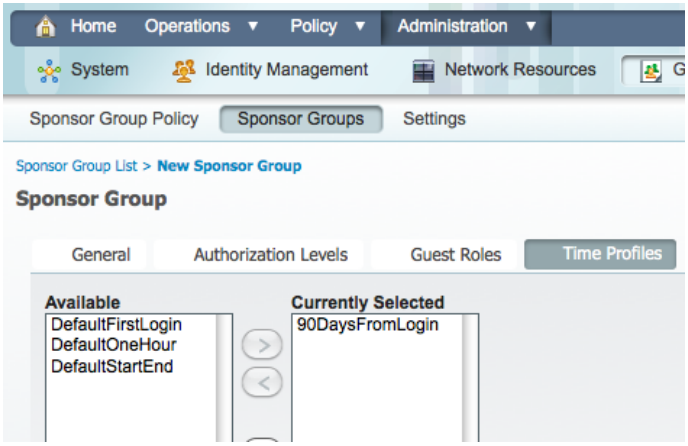
Step 7 From the Guest Roles tab, choose the contractor roles that the contractor sponsor group user is allowed to assign to the contractor user (Figure 14).

Figure 14 Setting Available Roles for Contractor Sponsor Group



Step 8 Under the Time Profiles tab, choose time profiles that the contractor sponsor group user is able to assign to contractor accounts (Figure 15).

Figure 15 Setting Available Time Profiles for the Contractor Sponsor Group



Step 9 Click Submit to save the configuration.

Procedure 6 Configure Identity Source Sequences for Sponsors (Optional)

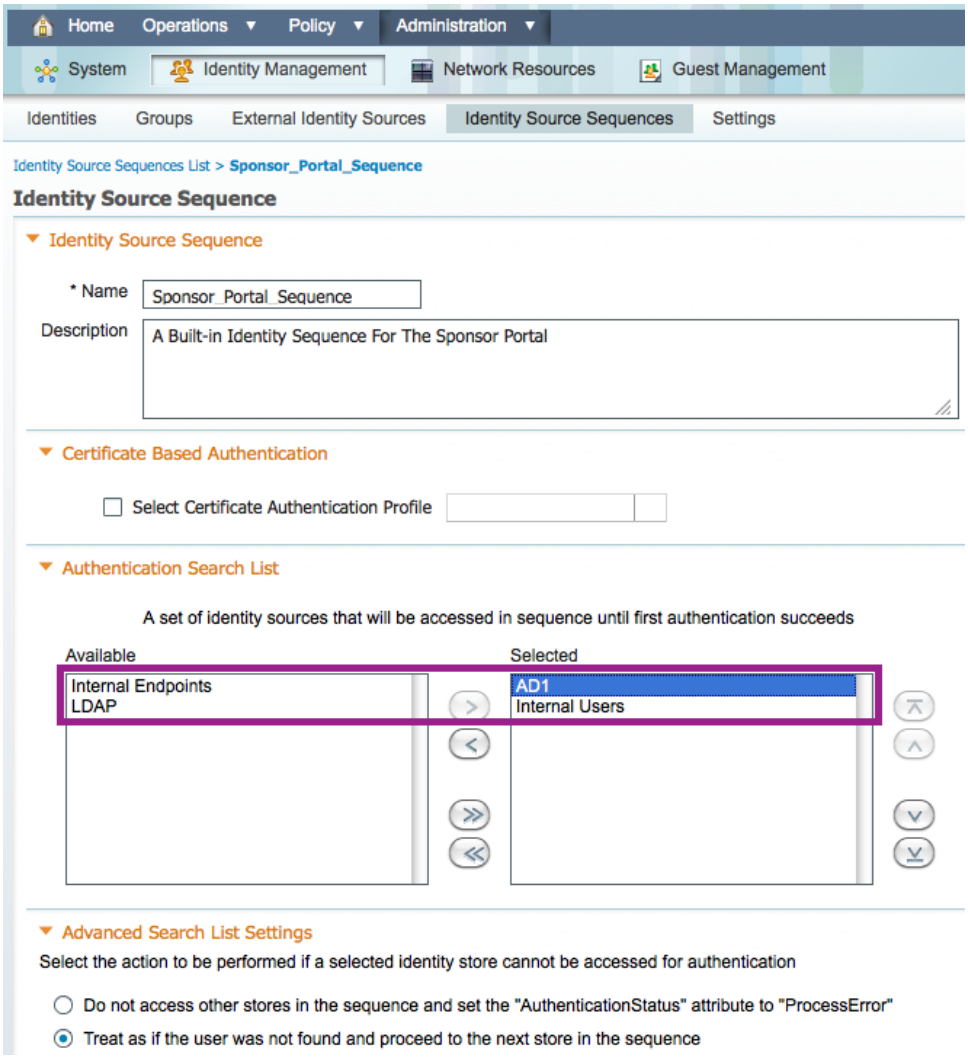
Identity source sequences define the order in which Cisco ISE will look for user credentials in the different databases. We will use the default identity sequence called Sponsor_Portal_Sequence. This one is sufficient for most installations.

Step 1 Navigate to Administration → Identity Management → Identity Source Sequences.

Step 2 Click Add to add an identity source sequence. You can check the check box or click Edit or Duplicate as needed.

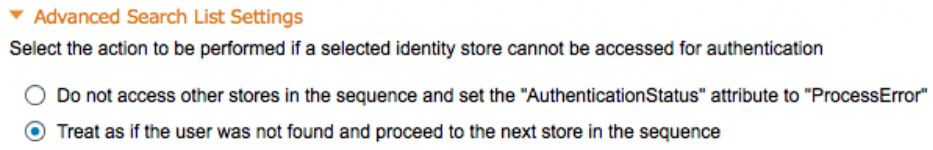
Step 3 The example in Figure 16 shows AD1, which is an Active Directory (AD) identity source.

Figure 16 Identity Source Sequence for Sponsor 1



Step 4 In the Authentication Search List area, select the appropriate option to indicate whether or not you want Cisco ISE to stop searching if the user is not found in the first identity store (Figure 17).

Figure 17 Identity Source Sequence for Sponsor 1



Procedure 7 Configure Identity Source Sequences for Guests (Optional)

We will use the default identity sequence called Guest_Portal_Sequence. We will add AD1 to the sequence, which allows AD domain users as well as ISE guest users to authenticate via Web Authentication.

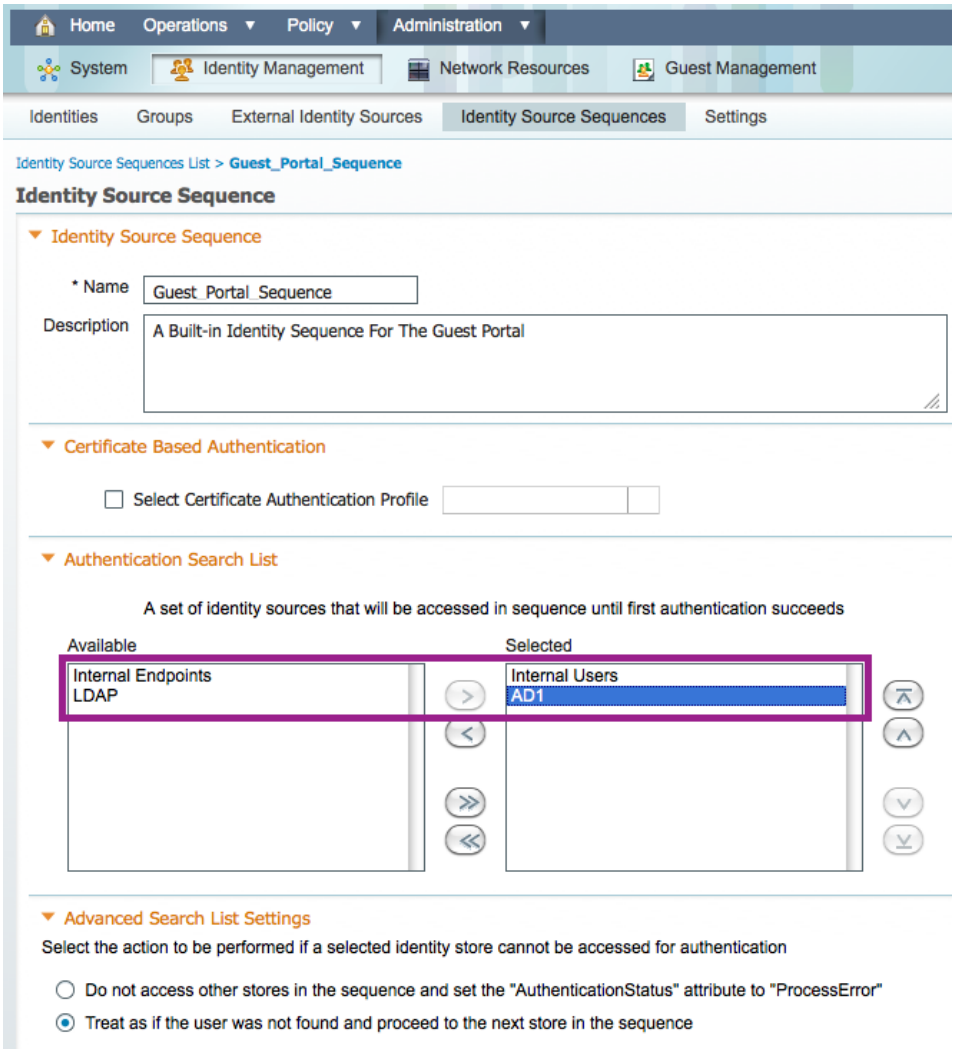
Step 1 Navigate to Administration → Identity Management → Identity Source Sequences.

Step 2 Click Add to add an identity source sequence. You can check the check box or click **Edit** or **Duplicate** accordingly (Figure 18).

The identity source sequence in Figure 18 shows an authentication order that checks the Internal database first, then AD1. Typically web access is used for guest and contract users, as employees should have a configured supplicant. By using this

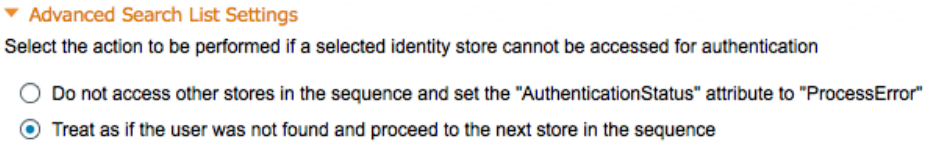
authentication order, guest authentication requests will be examined against the internal store first, and therefore will not be unnecessarily sent to AD servers.

Figure 18 Identity Source Sequence for Guest 1



Step 3 In the Authentication Search List area, select the appropriate option to indicate whether or not you want Cisco ISE to stop searching if the user is not found in the first identity store (Figure 19).

Figure 19 Identity Source Sequence 2



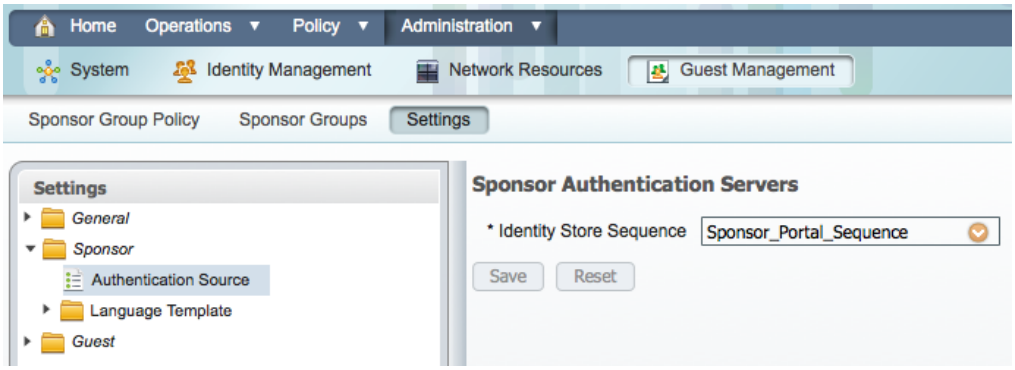
Procedure 8 Configure Authentication Sources for Sponsor Portal

To allow a sponsor to log in to the Sponsor portal, you have to choose an identity store sequence. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the Sponsor portal.

Step 1 Navigate to Administration → Guest Management → Settings → Sponsor → Authentication Source.

Step 2 From the Identity Store Sequence drop-down list, choose the sequence to be used for the sponsor authentication (**Sponsor_Portal_Sequence** in Figure 20).

Figure 20 Selecting the Identity Source Sequence for Sponsor Access



Step 3 Click Save.

Procedure 9 Configure a New Sponsor User (Optional)

For the majority of installations, Active Directory will be the identity source chosen to authenticate sponsors to. However, it is possible to create local sponsor users on ISE. This procedure details the creation of that local sponsor user.

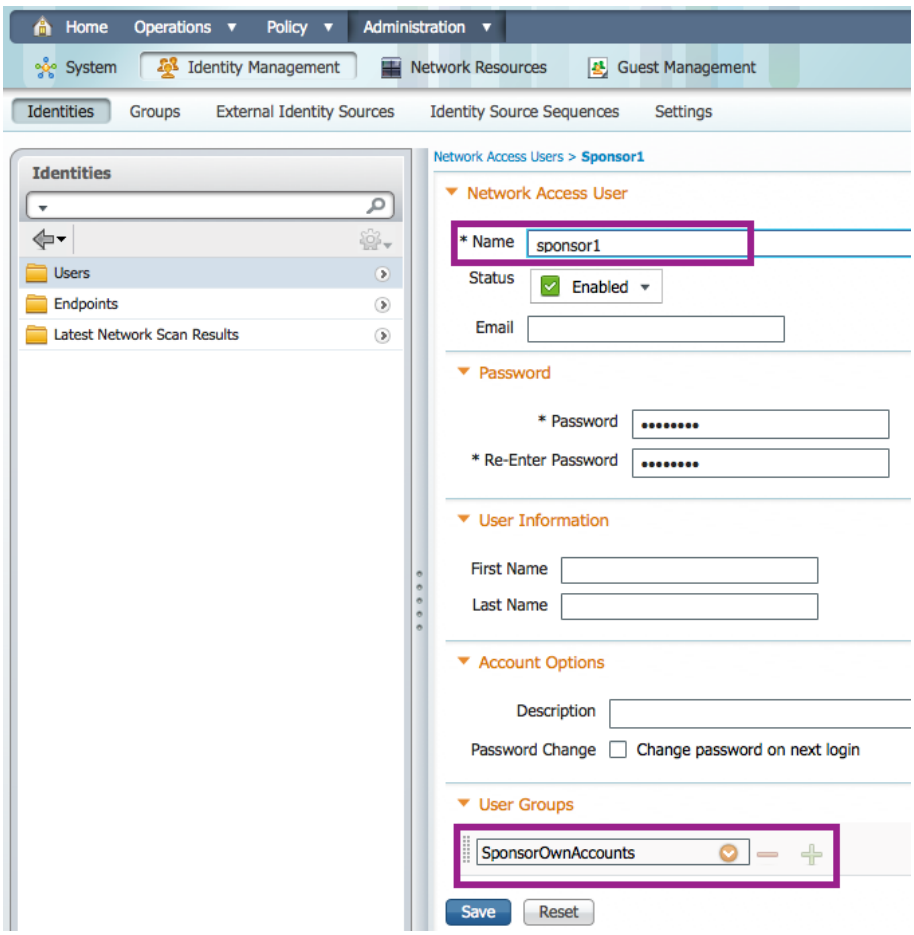
Step 1 Navigate to Administration → Identity Management → Identities → Users.

Step 2 Click Add to create a new network access user. The Network Access page is displayed.

Step 3 Enter values as appropriate to configure the sponsor user.

Step 4 Associate the sponsor with the appropriate sponsor user group (Figure 21).

Figure 21 Creating an ISE Internal Sponsor User



Step 5 Click Submit to add the user to the ISE database.

Procedure 10 Configure Sponsor Group Policies

Sponsor group policies are like identity mapping policies: they map identity groups (Active Directory or local groups) to a sponsor group. Each sponsor group may have different settings, such as the GuestSponsor and ContractorSponsor groups created in the "Configure Guest Sponsor Groups" and "Configure Contractor Sponsor Groups" procedures.

Step 1 Navigate to Administration → Guest Management → Sponsor Group Policy.

Step 2 Click Actions to insert a new rule above the existing rules.

Step 3 Name the rule ContractorSponsor (or GuestSponsor).

Step 4 Leave the Identity Groups at the default setting: Any**.**

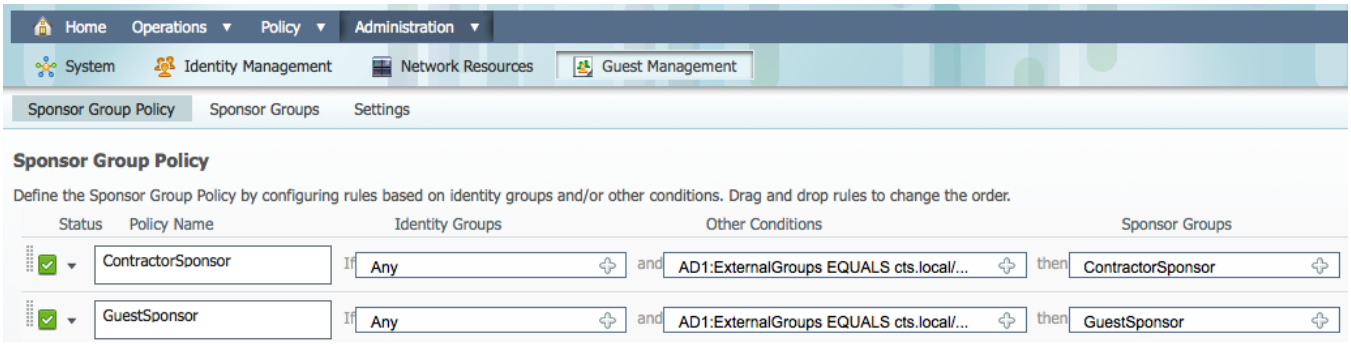
Step 5 Under conditions, select Create a New Condition (Advanced Option).

Step 6 Within the expression, choose: AD1 → ExternalGroups → Domain Admins (or Domain Users).

Step 7 Under Other Conditions, you may configure any number of conditions and statements per network requirements. These conditions will be used to match users as they authenticate to the Guest Sponsor portal.

Step 8 Under Sponsor Groups, choose **ContractorSponsor** (or **GuestSponsor**), which we created in an earlier procedures. Figure 22 shows the completed configuration.

Figure 22 Configuring Sponsor Group Policies



Step 9 Click Save to save configuration.

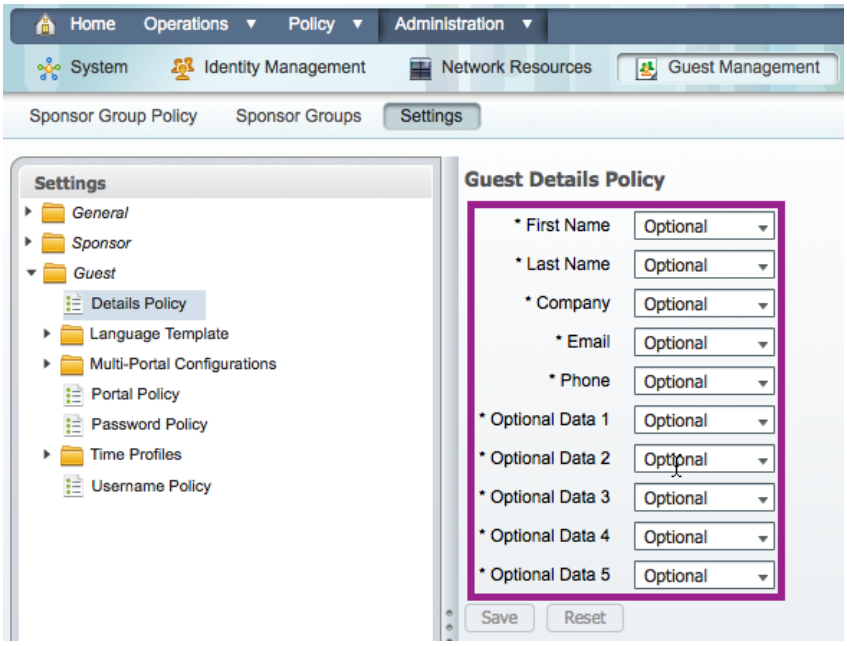
Procedure 11 Configure the Guest Details Policy

The details policy determines the data that the sponsor needs to enter when creating a guest account. The ISE administrator must define the fields that should appear on the Sponsor Guest Users page and in the Guest User Self-Registration page.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Details Policy.

Step 2 Specify one of the three settings for each field as required: Mandatory, Optional, or Unused (Figure 23).

Figure 23 Configuring the Guest Details Policy



Step 3 Click Submit.

Procedure 12 Configure the Guest Username Policy

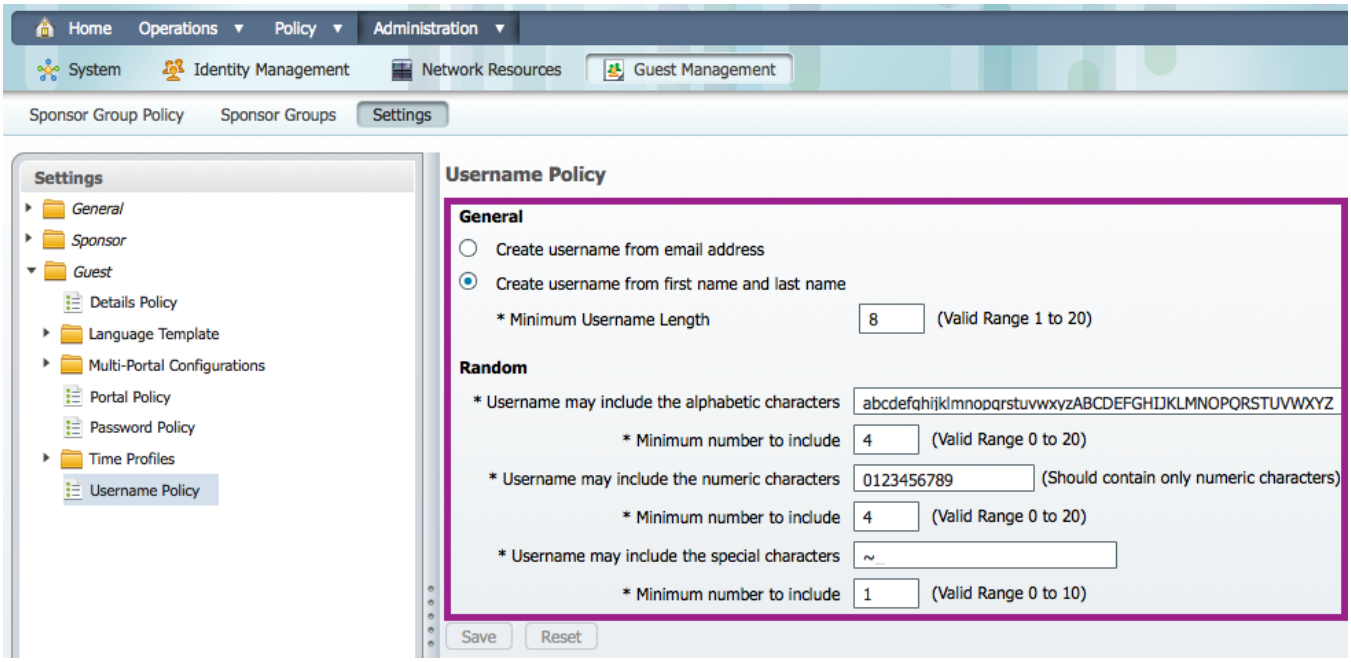
The Guest portal policy specifies how the usernames will be created for the guest accounts. It contains username requirements for guest services, such as allowed characters and the username format. Username policy configuration can be done in two ways: General or Random.

To configure general guest username policy, complete the following steps:

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Username Policy.

Step 2 Choose one of the username creation options: Create username from email address or Create username from first and last name (Figure 24).

Figure 24 Setting Guest Username Policy



Step 3 Enter minimum username length as required.

Step 4 Click Submit.

Procedure 13 Configure the Password Policy

The Guest portal policy specifies the characters that may be used for password generation, as well as how many characters of each type are required for all guest accounts.

Step 1 Navigate to Administration → Guest Management → Settings → Guest

Step 2 Password Policy (Figure 25).

Figure 25 Setting Guest Password Policy

Step 3 Enter appropriate details according to your guest password policy requirements.

Step 4 Click Submit.

Procedure 14 Configure the Options for the Guest Portal Policy

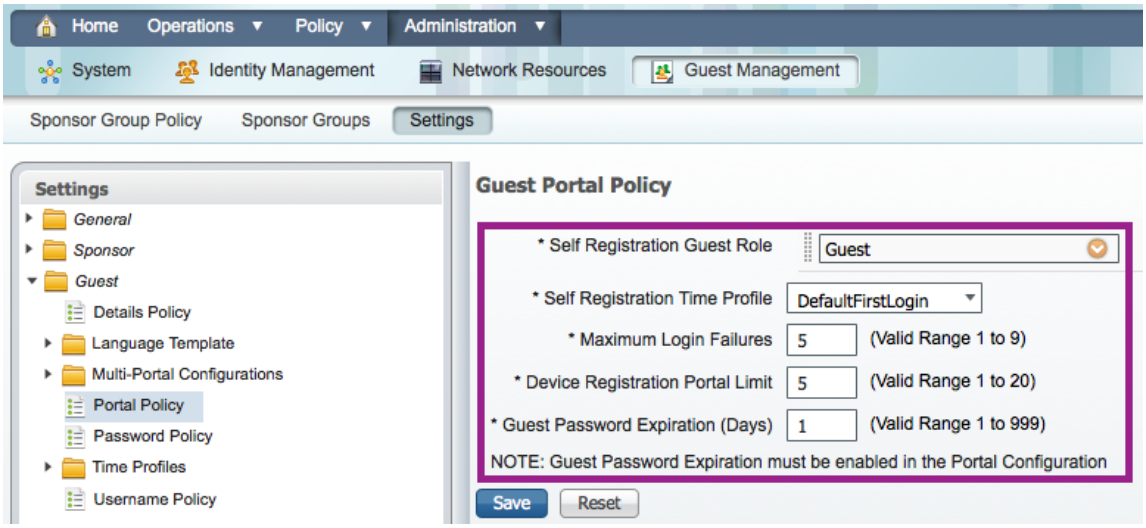
The Guest portal policy identifies functional items such as guest login attempts, password expiration, and so on.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Portal Policy.

Step 2 Configure the following options as required (see Figure 26):

- Self Registration Guest Role
- Self Registration Time Profile
- Maximum Login Failures
- Device Registration Portal Limit
- Guest Password Expiration

Figure 26 Guest Portal Policy Options



Step 3 Click Save to save configuration.

Universal Guest Configuration: Multi-Portal Guest User Configuration

A predefined DefaultGuestPortal is available under Multi-Portal Configurations. This portal has the default Cisco look-and-feel and you cannot customize it. To create a customized portal, you must first begin by adding a new portal.

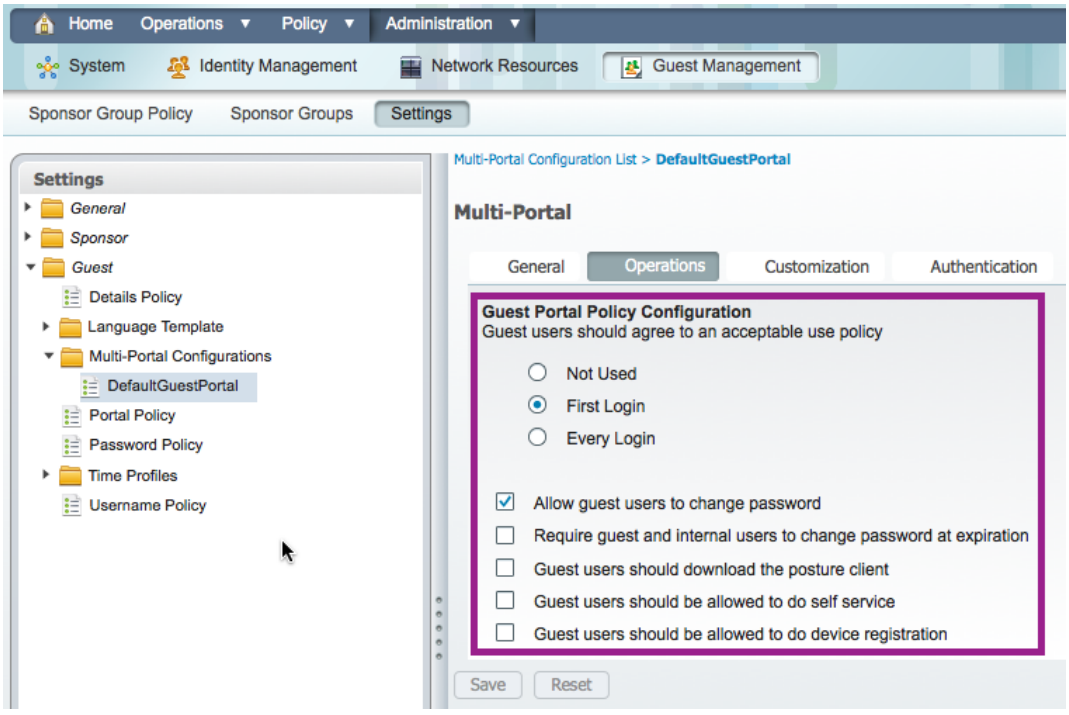
Procedure 1 Configure the Multi-Portal

This procedure is crucial to more than just guest access. It is critical that this portal be configured correctly for all Web Authentication needs.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Multi-Portal Configuration.

Step 2 Select the DefaultGuestPortal (Figure 27).

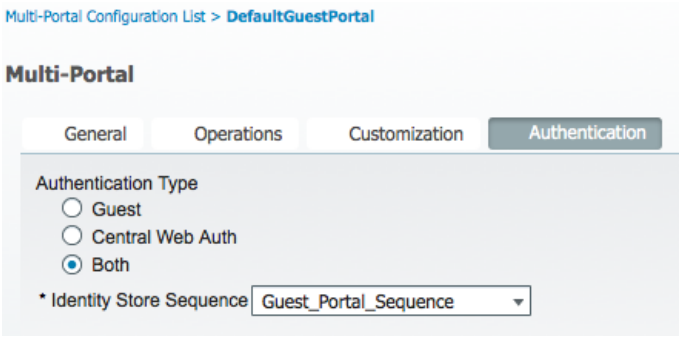
Figure 27 Default Guest Portal



Step 3 Make any changes to these settings as needed by your organization.

Step 4 Click the Authentication tab (Figure 28).

Figure 28 Default Guest Portal: Authentication



Step 5 Choose Both for the type of users who will be authenticated during the guest login.

Step 6 Select the Guest_Portal_Sequence identity store.

Step 7 Click Save.

Universal Guest Configuration: Configure Central Web Authentication

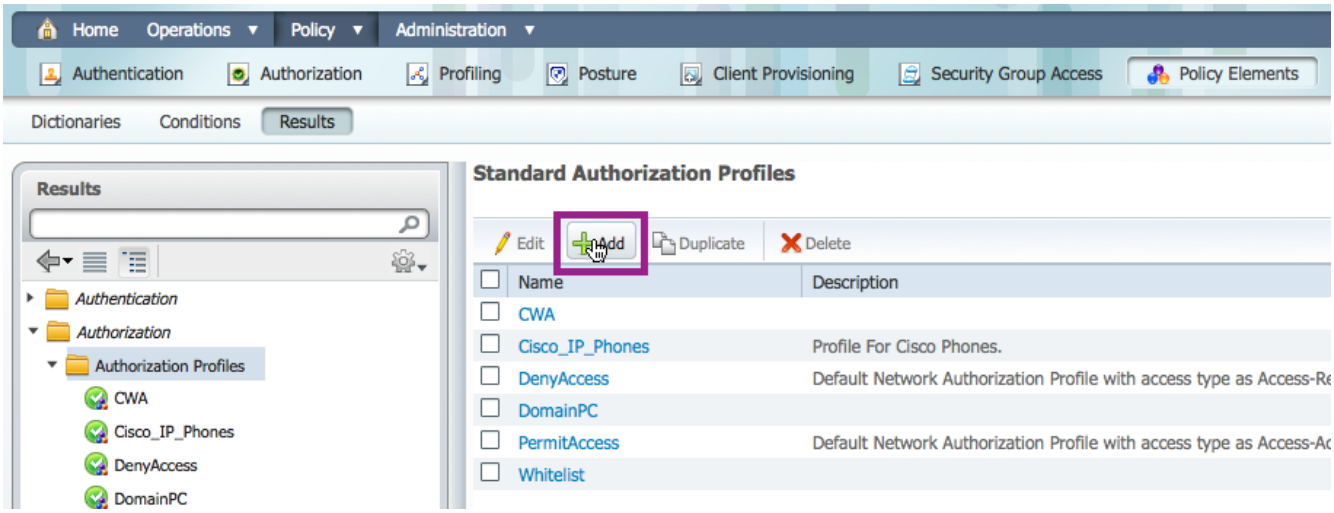
This procedure was described in detail in the HowTo-WebAuthentication_Design_Guide and enabled as part of the transition out of Monitor Mode into one of the end-state modes. We are including it here simply for reference.

Procedure 1 Create the Central Web-Auth AuthZ Profile

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click Add (Figure 29).

Figure 29 Creating Central Web-Auth (CWA) AuthZ Profile



Step 3 Name the AuthZ Profile **WEBAUTH.**

Step 4 Leave the Access Type as ACCESS_ACCEPT.

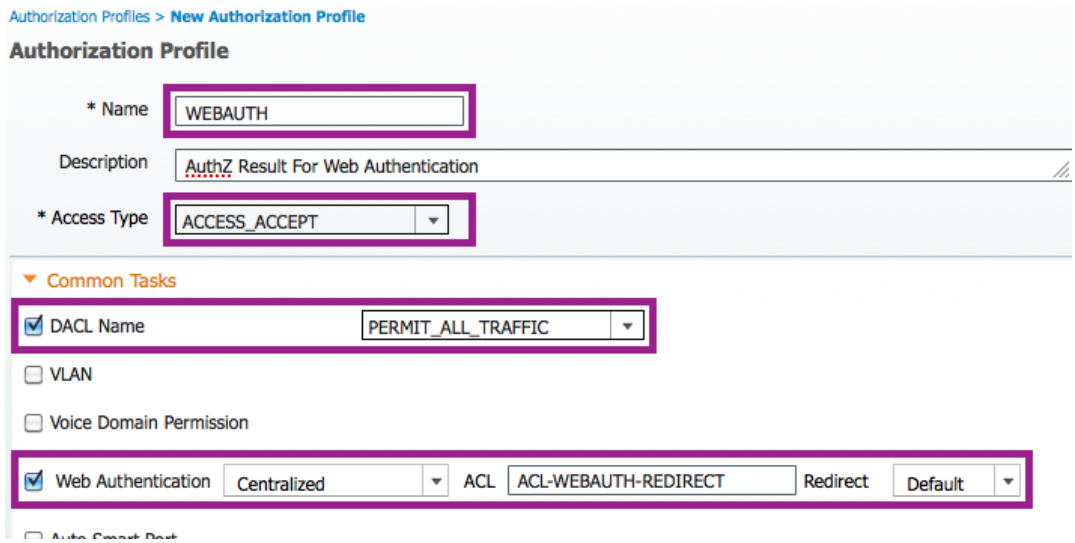
Step 5 Set the DACL to PERMIT_ALL_TRAFFIC .

Step 6 Enable Web Authentication, and enter **ACL-WEBAUTH-REDIRECT** as the ACL.

The ACL-WEBAUTH-REDIRECT ACL was built on the switch and the WLC in HowTo-WebAuthentication_Design_Guide. This is the ACL that identifies the "interesting traffic." Traffic matching that ACL will be redirected to the Centralized Web Authentication portal. This is distinctly different from a downloadable ACL that limits traffic through the port.

Step 7 Leave the Redirect as Default (Figure 30).

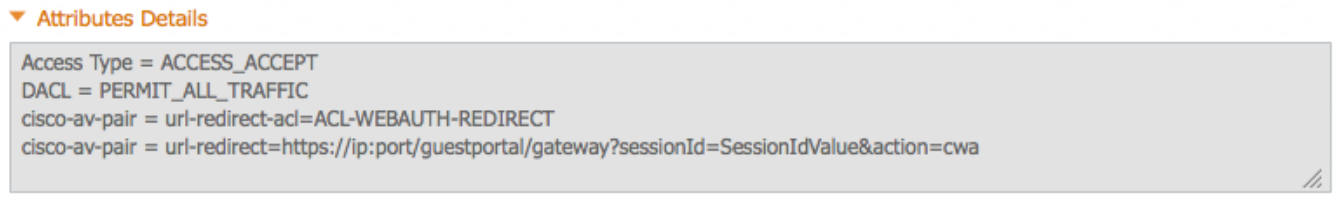
Figure 30 CWA AuthZ profile configuration



Step 8 Scroll to the bottom and check the Attributes Detail.

Step 9 Figure 31 shows the authorization profile for LAN switches. For an example showing the profile for the Cisco Wireless LAN Controller, see HowTo-WebAuthentication_Design_Guide.

Figure 31 Attribute Details



Step 10 Click Save.

Universal Guest Configuration: Configure Authorization for Guests and Contractors

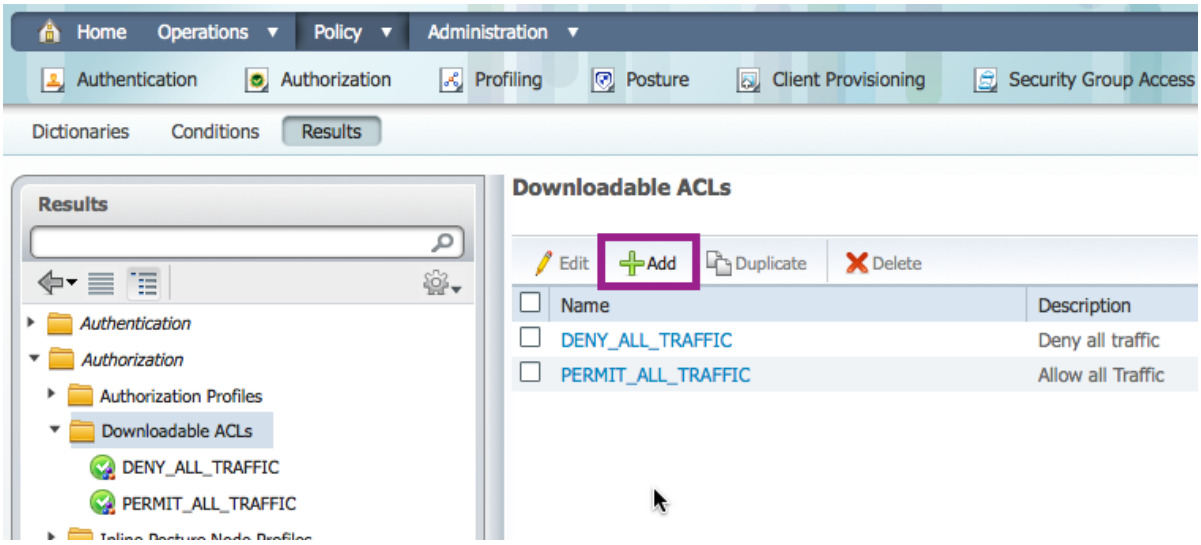
Authorization for guest users is a topic that could take up an entire design guide by itself. In this section, we will authorize the guest users into the Guest VLAN, and provide a downloadable ACL that permits all traffic ingress at the switch.

This type of AuthZ, which is commonly used, assumes the network infrastructure is providing the isolation of the guest user from the remainder of the corporate network. This type of isolation is often accomplished using network virtualization (virtual routing and forwarding [VRF] technology) or even simply access lists at the Layer 3 edge.

Procedure 1 Create a Downloadable ACL

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs (Figure 32).

Figure 32 Dynamic ACL



Step 2 Click Add.

Step 3 Configure the new dACL as described:

```
Name = GUEST
Description = dACL for GUEST users
DACL Content =  permit udp any host {DNS_Server}
deny ip any 10.0.0.0 0.255.255.255 (Internal resources)
permit ip any any
```

Step 4 Click Submit.

Step 5 Repeat Steps 1 through 4 with following dACL:

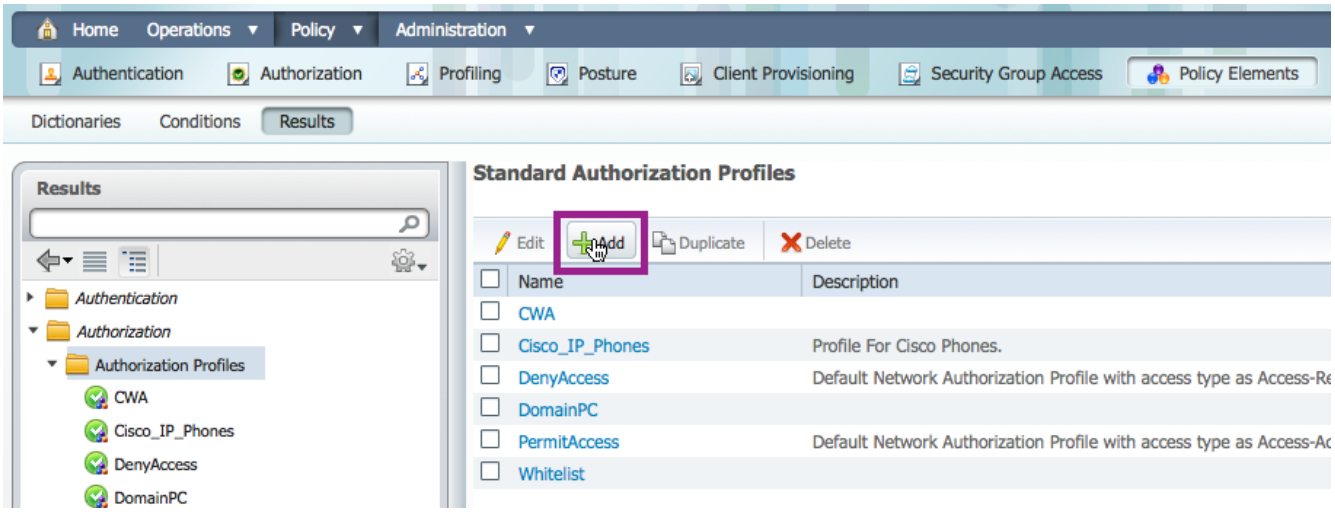
```
Name = CONTRACTOR
Description = dACL for CONTRACTOR users
DACL Content =  permit ip any any
```

Procedure 2 Create an AuthZ Profile

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click Add (Figure 33).

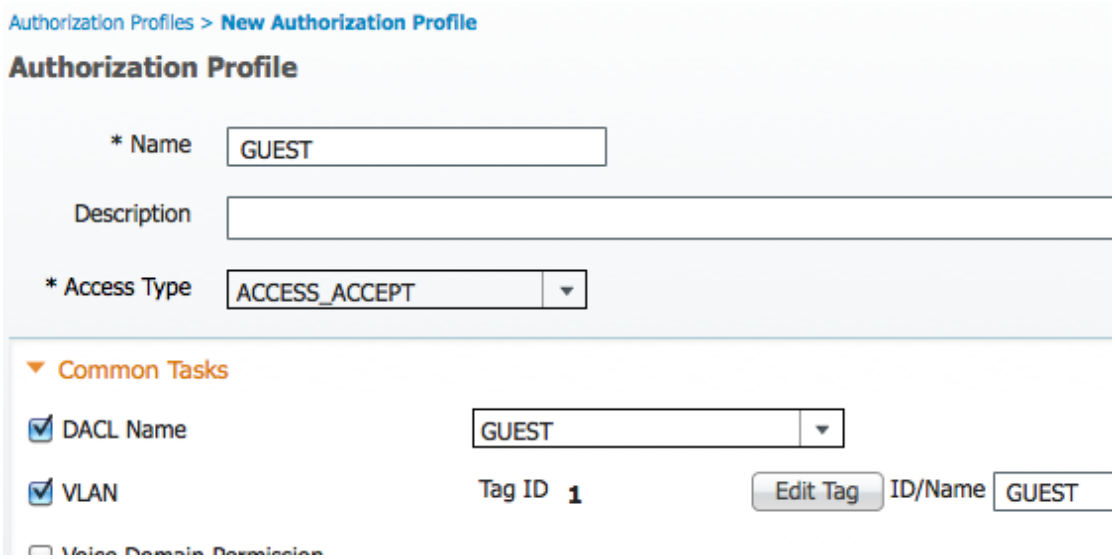
Figure 33 Create AuthZ profile for Each User Type



Step 3 Configure the new AuthZ Profile as described:

```
Name = GUEST
Description = AuthZ Profile for GUEST role (Authentication Mode)
Access-Type = ACCESS_ACCEPT
    --Common Tasks
DACL Name = GUEST
VLAN = GUEST
```

Figure 34 Guest AuthZ profile configuration



Step 4 Scroll to the bottom to check that the Attribute Details look like Figure 35, and click Submit.

Figure 35 Attribute Details

Step 5 Repeat Steps 1 through 4 with following attributes

```
Name = CONTRACTOR
Description = AuthZ Profile for CONTRACTOR role
```

```
Access-Type = ACCESS_ACCEPT
-- Common Tasks
DACL Name = CONTRACTOR
```

Step 6 Repeat Steps 1 through 4 with following attributes:

```
Name = EMPLOYEE
Description = AuthZ Profile for EMPLOYEE role
Access-Type = ACCESS_ACCEPT
-- Common Tasks
DACL Name = PERMIT_ALL_TRAFFIC
```

Step 7 Click Submit.

Procedure 3 Create a guest and contractor AuthZ policy rule

Step 1 Navigate to Policy → Authorization.

Step 2 Insert a new Rule above the Default rule (bottom of the Policy table).

Step 3 Name the new Rule **GUEST.**

Step 4 Under Identity Groups, click the plus sign on the picker.

Step 5 Choose User Identity Groups → GUEST.

Step 6 Leave Other Conditions alone.

Step 7 For Permissions, click the plus sign and select Standard → GUEST.

Step 8 Insert a new rule above the default rule (bottom of the Policy table).

Step 9 Name the new Rule **CONTRACTOR**.

Step 10 Under Identity Groups, click the plus sign on the picker.

Step 11 Choose User Identity Groups → CONTRACTOR

Step 12 Leave Other Conditions alone.

Step 13 For Permissions, click the plus sign, and select Standard → CONTRACTOR.

Step 14 Name the new Rule **EMPLOYEE-WEBAUTH**.

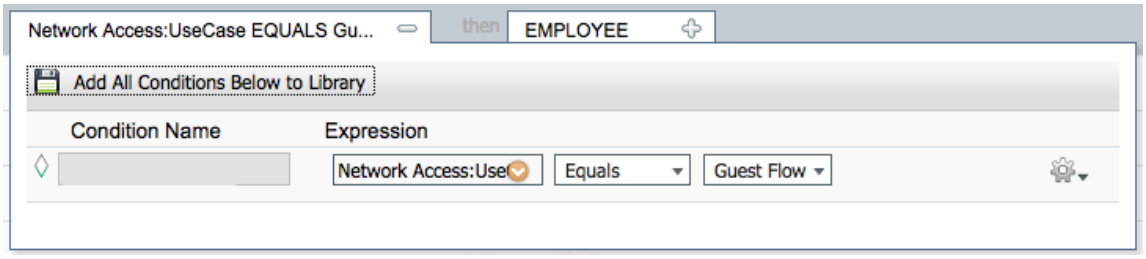
Step 15 Leave Identity Groups alone.

Step 16 Under Conditions, click the plus sign on the picker.

Step 17 Click Create New Condition.

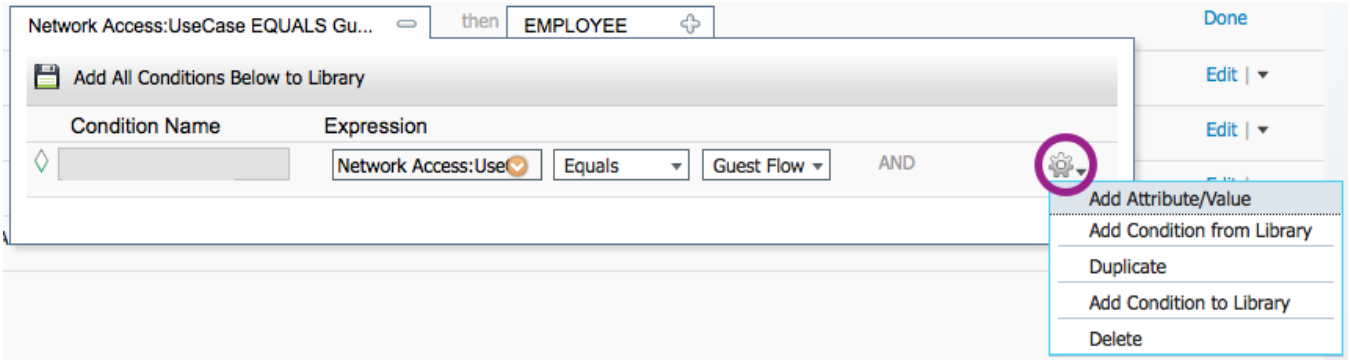
Step 18 Select Network Access → Usecase → Guest Flow (Figure 36).

Figure 36 Guest Flow Condition



Step 19 Click Add Attribute/ Value (Figure 37).

Figure 37 Add Additional Condition

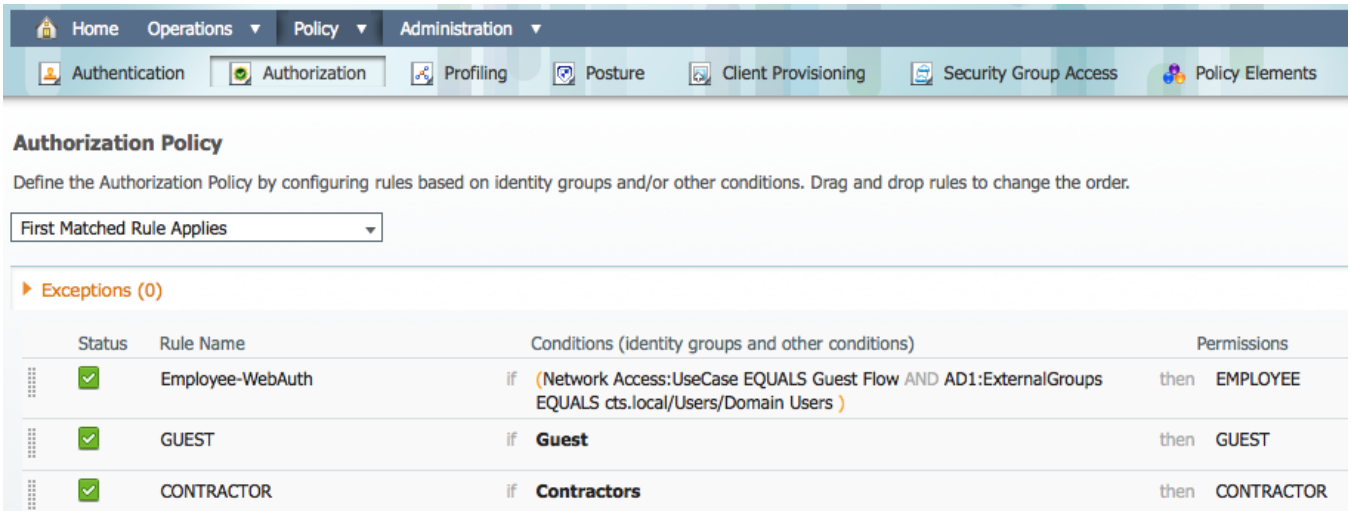


Step 20 Select AD1 → ExternalGroups → cts.local/Users/Domain Users.

Step 21 For Permissions, click the plus sign, and select Standard → EMPLOYEE.

Figure 38 shows the final authorization policy.

Figure 38 Final AuthZ Policy



Step 22 Click Save.

Universal Guest Configuration: Sponsor Login / Guest and Contractor Account Creation

A predefined DefaultGuestPortal is available under Multi-Portal Configurations. This portal has the default Cisco look-and-feel and you cannot customize it. To create a customized portal, you must first begin by adding a new portal.

Procedure 1 Configure Guest/Contractor User in the Sponsor Portal

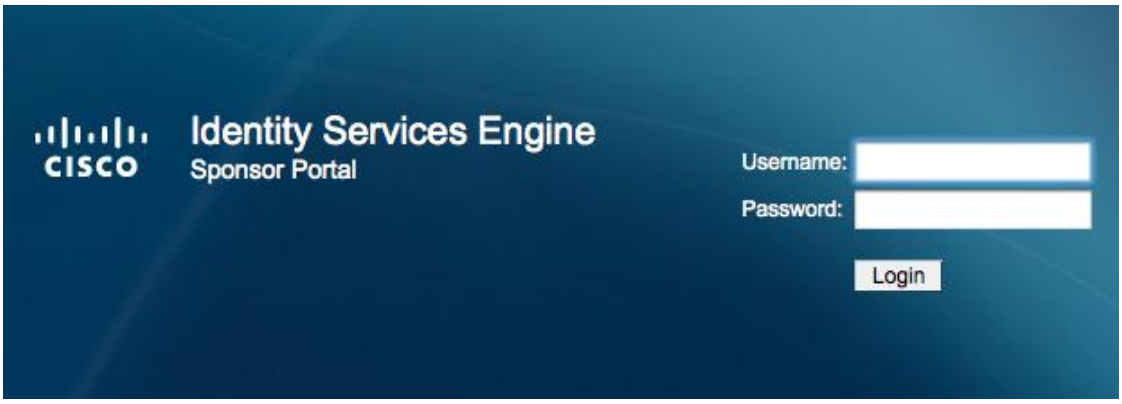
Step 1 From your web browser, navigate to the Sponsor portal at:

Step 2 **https://<portal_host_or_IP_address>:8443/sponsorportal**

Note: If you used the default sponsor URL option in the Sponsor User Configuration section, you can use a simple URL such as https://sponsor.cts.local here.

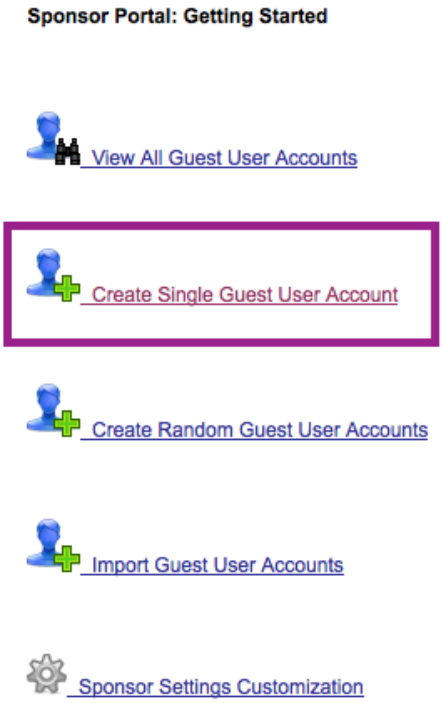
Step 3 Log in to the portal using the sponsor user's credentials (Figure 39).

Figure 39 Sponsor Portal Login



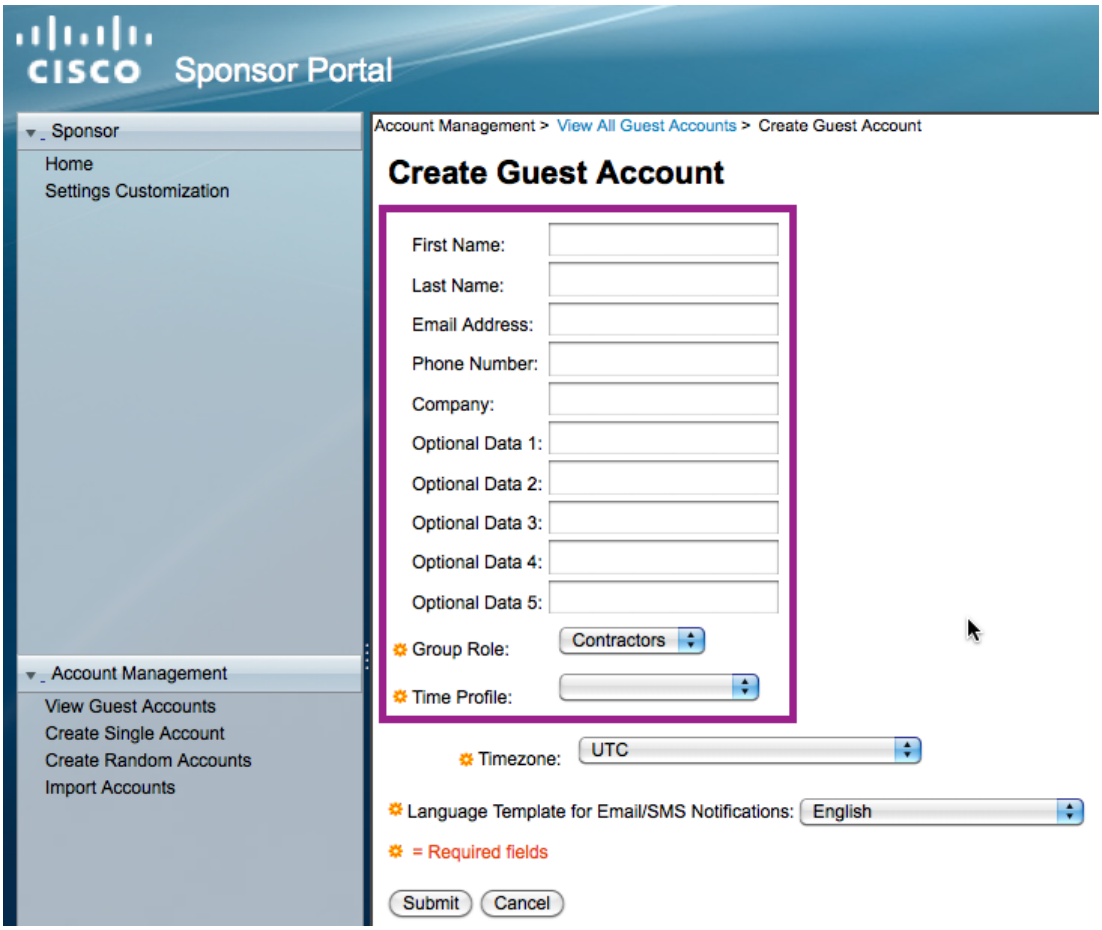
Step 4 Navigate to Create Single Guest User Account (Figure 40).

Figure 40 Sponsor Portal



Step 5 Configure the required fields (Figure 41).

Figure 41 Creating Guest Account from Sponsor Portal



Step 6 Click Submit.

Appendix A: References

Cisco TrustSec System:

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html